OWASP AppSec Pipeline

Table of Contents

[1 Overview 2](#_Toc1218580778)

[1.1 What is OWASP AppSec Pipeline? 3](#_Toc822978679)

[1.2 Why automate security? 3](#_Toc463136041)

[1.3 What tools can you use? 3](#_Toc112660956)

[1.4 Getting started with OWASP AppSec Pipeline: 3](#_Toc875350948)

[2 References 4](#_Toc857067336)

# Overview

Imagine a nimble fleet of security dragonflies constantly flitting around your software, identifying and resolving vulnerabilities before they can take flight. That's the essence of the OWASP AppSec Pipeline, a framework for automating and integrating security throughout your development lifecycle.

## What is OWASP AppSec Pipeline?

It's not just a single tool, but a collective effort, offering resources and best practices to build your own custom security pipeline. Think of it as a blueprint for assembling your dragonfly squadron, tailored to your specific needs and workflow.

## Why automate security?

* Faster and more efficient: Automated tools scan and analyze code continuously, catching vulnerabilities early and preventing costly fixes later.
* Reduced human error: Manual security checks are prone to fatigue and oversights, while automated tasks are precise and consistent.
* Improved team collaboration: Everyone involved in the development process is kept informed about security risks and mitigation strategies.
* Continuous security mindset: Building security into every stage of development fosters a culture of proactive risk management.

## What tools can you use?

The AppSec Pipeline is flexible and allows you to incorporate various security tools depending on your needs. Some popular options include:

* Static Application Security Testing (SAST): Analyzes source code for vulnerabilities without actually running it.
* Software Composition Analysis (SCA): Checks for known vulnerabilities in third-party libraries and dependencies.
* Dynamic Application Security Testing (DAST): Simulates attacks to discover vulnerabilities in an active application.
* Interactive Application Security Testing (IAST): Instruments the application to detect runtime attacks and suspicious behavior.
* Infrastructure Scanning: Secures your underlying infrastructure and cloud environments.

## Getting started with OWASP AppSec Pipeline:

* Identify your goals: What are your specific security needs and challenges?
* Choose your tools: Select the right tools based on your goals and development environment.
* Integrate into your workflow: Seamlessly connect security testing with your existing development and continuous integration/continuous delivery (CI/CD) pipelines.
* Monitor and iterate: Continuously evaluate your pipeline's effectiveness and adapt it as needed.

# References

1. <https://owasp.org/www-pdf-archive/OWASP_Tampa_-_02_19_2016_-_AppSec_Pipeline.pdf>
2. <https://www.youtube.com/watch?v=3PgWM8qwWas>